(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 3 139 649 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
08.03.2017 Bulletin 2017/10

(51) Int Cl.:
H04W 12/06 *(2009.01)* ***H04L 29/06*** *(2006.01)*

(21) Application number: **15306361.5**

(22) Date of filing: **04.09.2015**

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Designated Extension States:
BA ME
Designated Validation States:
MA

(71) Applicant: **GEMALTO SA**
92190 Meudon (FR)

(72) Inventors:
- **PAULIAC, Mireille**
  13881 GEMENOS Cedex (FR)
- **PRADEN, Anne-Marie**
  13881 GEMENOS Cedex (FR)

(74) Representative: **Scheer, Luc et al**
Gemalto SA
525, Avenue du Pic de Bertagne
CS 12023
13881 Gémenos Cedex (FR)

(54) METHOD TO AUTHENTICATE A SUBSCRIBER IN A LOCAL NETWORK

(57) The present invention relates to a method to authenticate a subscriber (IMSIi) within a local network (LNj) comprising preliminary step of deriving a subscriber key (SMKi) in local keys (LKi), one local key (LKiLNj) for each local network (LNj) the subscriber (IMSIi) is authorized to access, provisioning each local network (LNj) the subscriber (IMSIi) is authorized to access with its own local key (LKiLNj). When an authentication is required in a given local network (LNj), an UICC application derives a local key (LKiLNj) in the UICC application of the subscriber (IMSIi) using the network identifier (LNj), the key derivation function (KDF) and the subscriber key (SMKi) and use the derived local key (LKiLNj) in the algorithm to perform local authentication in the local network (LNj).

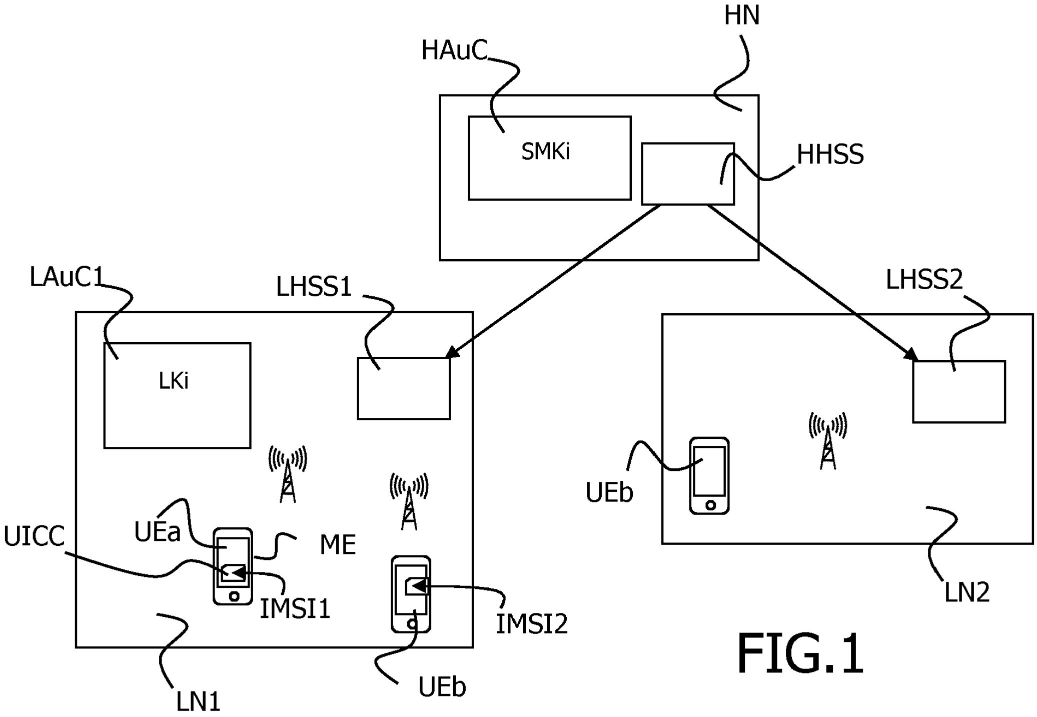

FIG.1

Printed by Jouve, 75001 PARIS (FR)

Description

FIELD OF THE INVENTION

[0001] The present invention relates to a method to authenticate a subscriber within a local network, without requiring online communication between this local network and the home network of the subscriber.

[0002] A local network is defined as a network distinct from the home network in which the subscriber is registered.

[0003] The invention also pertains to an authentication center of a home subscriber server (HSS) hosted by a home operator and to an UICC application.

BACKGROUND OF THE INVENTION

[0004] 3GPP addresses new scenarios where the operator's subscriber shall be authenticated within local E-UTRAN network (4G), without communication with the home network. The scenarios are for commercial use or for public safety, notably when the macro network is not available.

[0005] The operator has interest in keeping the control of the authentication of his subscriber within local networks. The subscriber should not be allowed to be authenticated within a local network deployed without agreement with the home operator of the subscriber.

[0006] Solutions to authenticate a subscriber within any local network relying on one unique key shared between the home HSS, the UICC application and all the local networks may have a security issue in case that a local HSS would be hosted in less secure environment than the home HSS. In such a scenario, it may happen that an attacker could have physical access to the local HSS and retrieve the unique key used to authenticate the subscriber. Consequently, all the other local networks using the same key to authenticate the subscriber would be known.

[0007] A synchronization issue may also exist, in case of 3GPP authentication, there is the use of Sequence Number (SQN) mechanism. Using the same SQN within different local networks not connected to synchronize could end in de-synchronization of the UICC in some scenarios. Then authentication could fail and additional process may be required.

[0008] Further alternative and advantageous solutions would, accordingly, be desirable in the art.

SUMMARY OF THE INVENTION

[0009] The present invention aims at proposing a novel scheme of authentication where no on-the-fly communication between the local and the home network occurs.

[0010] The present invention is defined, in its broadest sense, as a method comprising the preliminary steps of, for a home authentication center (AuC) of a home subscriber server (HSS) hosted in a home network:

- storing a subscriber key (Kmacro) per subscriber in the home authentication center, said home authentication center having a key derivation function (KDF) and said subscriber key being dedicated to the authentication of this subscriber within any local network having an agreement with the home operator,
- deriving the subscriber key in local keys, one local key for each local network the subscriber is authorized to access,
- provisioning each local network the subscriber is authorized to access with its own local key,
- provisioning an UICC application of the subscriber with the subscriber key and the key derivation function (KDF),
- provisioning the UICC application of the subscriber with an algorithm to perform local authentication,

said method further comprising the steps of, when an authentication is required in a given local network, for the UICC application:

- receiving a network identifier,
- deriving a local key in the UICC application of the subscriber using the network identifier of the local network, the key derivation function and the subscriber key,
- using the derived local key in the algorithm to perform local authentication in the local network.

[0011] This invention relies on the generation of local keys, both in the operator network and in the user equipment of the operator's subscriber, to perform AKA authentication of the subscriber within a local E-UTRAN network.

[0012] The home network sends a local key to any local E-UTRAN network where a subscriber is authorized to be present and could be authenticated locally thanks to AKA authentication. One local key is dedicated to only one local network.

[0013] The invention allows an operator to continue using AKA algorithm to authenticate his subscribers within local networks. It thus allows the home operator to keep control within local networks. The authentication takes place only if the local authentication center AuC and the user equipment are provisioned with keys provided by the home operator. The use of local keys, specific to only one local network, provides a high level of security. This feature is important in case that a local authentication center AuC would be more vulnerable to attacks, than a home authentication center AuC, including the one in the local HSS. If an attacker has access to one local authentication center AuC, the retrieved local keys could not be used for authentication within others local networks.

[0014] The invention has also the advantage to allow local authentication based on symmetric keys. It further guarantees that UICC-based authentication will take place when the subscriber is within local networks. Since

AKA-based authentication shall be hosted in a UICC, while certificate-based solutions can be hosted in the terminal part of the user equipment.

[0015] The authentication method used in the local network, i.e. AKA authentication with AUTN, RAND, can be the standard one and no modification are needed neither within the local network, neither in the UICC.

[0016] The UICC will only contain additional files or dedicated application to store the new subscriber key and all the derived local keys for all local networks.

[0017] Associated OTA services are advantageously implemented to update the list of authorized local networks.

[0018] According to an advantageous feature, said method comprising, as a preliminary step, a step of, for the authentication center, provisioning the UICC application of the subscriber with a list of identifiers of local networks where the subscriber is authorized to access, and, when an authentication is required in a given local network, for the UICC application, a step of checking the presence of the local network's identifier in the list.

[0019] With this feature it is necessary for the UICC application to further contain the list of authorized local networks where the subscriber would be authorized to be present.

[0020] According to an advantageous implementation, once the local key is derived by the UICC application, the method further comprises the step of storing the local key for this local network and the step of checking the presence of a stored local key for the local network's identifier.

[0021] This feature avoids to re-iterate the key derivation each time the UICC enters a local network.

[0022] According to a specific implementation, the authentication process using a sequence number mechanism, it further comprises the step of, for the authentication center and for the UICC application, while deriving local keys, associating an local array of sequence numbers to each derived local key.

[0023] Such an array of sequence numbers is typically associated to some standard authentication process. The invention is fully compatible with such standards.

[0024] The invention further relates to an authentication center of a home subscriber server hosted in a home network, said authentication center storing a subscriber key per subscriber application, said subscriber key being dedicated to the authentication of a subscriber within any local networks having an agreement with home network's operator, said authentication center having a key derivation function to derive the subscriber key in local keys, one for each local network the subscriber is authorized to access, said authentication center having provisioning resources to provision each local network the subscriber is authorized to access with its own local key, and to provision UICC of subscriber with own subscriber key, with key derivation function (KDF) and with an algorithm to perform local authentication.

[0025] Such an authentication center enables the implementation of the invention on the side of the home network.

[0026] The invention at last relates to an UICC application provided with a subscriber key, said subscriber key being dedicated to the authentication of a subscriber within any local networks having an agreement with the home network, a key derivation function (KDF) and an algorithm to perform local authentication, said UICC application being further adapted to receive a network identifier from a local network and to use this network identifier, the key derivation function and the subscriber key to derive a local key in the UICC application of the subscriber, the UICC application further being adapted to use the derived local key in the algorithm to perform local authentication in the local network.

[0027] Such an UICC application enables the implementation of the invention on the user equipment side.

[0028] To the accomplishment of the foregoing and related ends, one or more embodiments comprise the features hereinafter fully described and particularly pointed out in the claims.

BRIEF DESCRIPTION OF THE DRAWINGS

[0029] The following description and the annexed drawings set forth in detail certain illustrative aspects and are indicative of but a few of the various ways in which the principles of the embodiments may be employed. Other advantages and novel features will become apparent from the following detailed description when considered in conjunction with the drawings and the disclosed embodiments are intended to include all such aspects and their equivalents.

- Figure 1 represents the environement in which the invention is implemented;
- Figure 2 shows a functional diagram of the exchanges between entities according to the method of the invention.

DETAILED DESCRIPTION OF EMBODIMENTS OF THE INVENTION

[0030] For a more complete understanding of the invention, the invention will now be described in detail with reference to the accompanying drawings. The detailed description will illustrate and describe what is considered as a preferred embodiment of the invention. It should of course be understood that various modifications and changes in form or detail could readily be made without departing from the spirit of the invention. It is therefore intended that the invention may not be limited to the exact form and detail shown and described herein, nor to anything less than the whole of the invention disclosed herein and as claimed hereinafter. The same elements have been designated with the same references in the different drawings. For clarity, only those elements and steps which are useful to the understanding of the present invention have been shown in the drawings and will be described.

[0031] Figure 1 schematically shows an environment comprising a home network HN and two local networks LN1 and LN2. Each of them has a respective home subscriber server HHSS, LHSS1 and LHSS2 and an authentication center HAuC, LAuC1, LAuC2. HSS are accessible for base stations in their corresponding local networks.

[0032] It is here noted that a user equipment UE consists of an UICC having UICC Application with IMSIi associated to the subscription of the user and a mobile equipment ME. IMSIi is an identifier of the subscriber for one specific UICC Application. If several UICC applications are present in the UICC, each UICC application can have a dedicated IMSI. Nothing prevents to have several UICCs within a UE.

[0033] User equipments UEa and UEb respectively have IMSI1 in a UICC application and IMSI2 in UICC application, said IMSIi originating from home network HN. It is here further noted that reference "IMSI" is used to designate the identity of the subscriber according to the UMTS terminology. Any other kind of identity is concerned as IMPI (IMS) and others.

[0034] User equipments UEa and UEb are susceptible to enter in communication with base stations of local networks LNj for example in a situation where the UEa and UEb can no longer communicate with normal network. In such a situation, the subscriber needs to be authenticated within the local network LNj without any contact with the home operator.

[0035] For this purpose, the invention proposes that the authentication center HAuC of the home network HN stores preliminarily a subscriber key SMKi per subscriber i, and possibly a random value RANDi to be optionally used in the derivation function. Said subscriber key SMKi is dedicated to the authentication of the subscriber associated to the IMSIi in a UICC application within any local network having an agreement with the home operator HN.

[0036] According to the invention, the authentication center AuC has a key derivation function to derive local keys from the subscriber key SMK. A local key LKi_{LNj} per local network LNj having an agreement with the home operator is thus obtained. This local key LKi_{LNj} is then sent to the HSS of the concerned local network LNj as shown on figure 2 for local network LN1. A local key is sent for each subscriber i susceptible and authorized to enter in local network LNj. The local authentication center LAuCj stores all these local keys LKi_{LNj}.

[0037] In case of 3GPP AKA authentication, the AuC of the home HHSS sends to the local HSS LHSSj the array of Sequence Number (SQN) associated to each local key LK. It stores all these keys, one per subscriber and, in case of 3GPP AKA authentication, the local authentication center LAuC also contains the array of Sequence Number (SQN) associated to each local key LK.

[0038] The subscriber key SMKi, the derivation function KDF,an algorithm to perform local authentication, e. g. 3GPP AKA authentication (Milenage), and possibly the random value RANDi, are then provisioned at the UICC of the user equipment UEa, in an UICC application with IMSI1. This step ends the preliminary steps PrS of the invention which necessitates dedicated communications with the UICC of the subscriber IMSIi when it is in the field of the home network.

[0039] Further, the UICC application contains a list of local networks LNj where the subscriber i is authorized to be. The operator of the home network could update this list of authorized local network when the UE with UICC containing the UICC application with IMSIi was or is again in the field of home network.

[0040] Then, when the local network LN1 initiates a mutual authentication with the UICC application with IMSI1 of the user equipment UEa in the local network, LN1 in figure 2, the user equipment UEa receives a local network identifier Id(LN1) that it provides to the UICC application with IMSI1, e.g. USIM.

[0041] When the identifier Id(LN1) is not in the list of authorized networks, the authentication fails. When the identifier Id(LN1) is in the list of authorized networks, selection of the corresponding local network key $SMK1_{LN1}$ and the activation of the derivation function KDF to obtain the local key $LK1_{LN1}$ for the identified local network LN1 are triggered.

[0042] The invention can be implemented in such a way that, if a local key has already been derived for the user equipment, the local HSS LHSS1 keeps the local key in memory. In this case, when the network is listed, the UICC application subsequently checks if a local key was previously calculated. In such a case, the derivation is not done again and the stored local key associated to the concerned network is used.

[0043] Otherwise, the derivation is in fact triggered. Each local key is specific per subscriber to one local network. The derivation of the local key is linked to the identity IMSI1 of the subscriber and the identity of the local network Id(LN1), thus:

$LK1_{LN1}$ = KDF (SMK1, "local-aka", RAND1, IMSI1, Id(LN1)).

[0044] The obtained local key can be stored depending on the implementation. In case of AKA-based authentication, as specified by 3GPP, an array of Sequence Number (SQN) is associated to each local key LK.

[0045] The local key $LK1_{LN1}$ is then used in secure authentication Aut($LK1_{LN1}$) with the LHSS1 of the local network LN1. AKA authentication is preferably used.

[0046] According to the invention, the UICC application stores the following triplets:

Id(LNj), $LK1_{LNj}$, SQNj for as many j as concerned networks.

[0047] In the above detailed description, reference is made to the accompanying drawings that show, by way of illustration, specific embodiments in which the invention may be practiced. These embodiments are described in sufficient detail to enable those skilled in the art to practice the invention. The above detailed description is, therefore, not to be taken in a limiting sense, and the scope of the present invention is defined only by the appended claims, appropriately interpreted, along with the full range of equivalents to which the claims are entitled.

Claims

1. Method to authenticate a subscriber (IMSIi) within a local network (LNj) comprising the preliminary steps of, for a home authentication center (HAuC) of a home subscriber server (HHSS) hosted in a home network (HN):

   - storing a subscriber key (SMKi) per subscriber (IMSIi) in the home authentication center (HAuC), said home authentication center (HAuC) having a key derivation function (KDF) and said subscriber key (SMKi) being dedicated to the authentication of this subscriber (IMSIi) within any local network (LNj) having an agreement with the home operator (HN),
   - deriving the subscriber key (SMKi) in local keys (LKi), one local key (LKi_{LNj}) for each local network (LNj) the subscriber (IMSIi) is authorized to access,
   - provisioning each local network (LNj) the subscriber (IMSIi) is authorized to access with its own local key (LKi_{LNj}),
   - provisioning an UICC application of the subscriber (IMSIi) with the subscriber key (SMKi) and the key derivation function (KDF),
   - provisioning the UICC application of the subscriber (IMSIi) with an algorithm to perform local authentication,

   said method further comprising the steps of, when an authentication is required in a given local network (LNj), for the UICC application:

   - receiving a network identifier (Id(LNj)),
   - deriving a local key (LKi_{LNj}) in the UICC application of the subscriber (IMSIi) using the network identifier (LNj) of the local network, the key derivation function (KDF) and the subscriber key (SMKi),
   - using the derived local key (LKi_{LNj}) in the algorithm to perform local authentication in the local network (LNj).

2. Method according to claim 1, said method comprising, as a preliminary step, a step of, for the authentication center (HAuC), provisioning the UICC application of the subscriber (IMSIi) with a list of identifiers of local networks (Id(LNj)) where the subscriber (IMSIi) is authorized to access, and, when an authentication is required in a given local network (LNj), for the UICC application, a step of checking the presence of the local network's identifier (Id(LNj)) in the list.

3. Method according to one of claims 1 and 2, wherein, once the local key (LKi_{LNj}) is derived by the UICC application, the method further comprises the step of storing the local key (LKi_{LNj}) for this local network (LNj) and the step of checking the presence of a stored local key (LKi_{LNj}) for the local network's identifier (Id(LNj)).

4. Method according to one of preceding claims, wherein, the authentication process using a sequence number mechanism, it further comprises the step of, for the authentication center (HAuC) and for the UICC application, while deriving local keys (LKi_{LNj}), associating an local array of sequence numbers to each derived local key (LKi_{LNj}).

5. Authentication center (HAuC) of a home subscriber server (HHSS) hosted in a home network (HN), said authentication center (HAuC) storing a subscriber key (SMKi) per subscriber application, said subscriber key (SMKi) being dedicated to the authentication of a subscriber (IMSIi) within any local networks (LNj) having an agreement with home network's operator, said authentication center (HAuC) having a key derivation function (KDF) to derive the subscriber key (SMKi) in local keys (LKi_{LNj}), one for each local network (LNj) the subscriber (IMSIi) is authorized to access, said authentication center (HAuC) having provisioning resources to provision each local network (LNj) the subscriber (IMSIi) is authorized to access with its own local key (LKi_{LNj}), and to provision UICC application of subscriber (IMSIi) with own subscriber key (SMKi), with key derivation function (KDF) and with an algorithm to perform local authentication.

6. UICC application provided with a subscriber key (SMKi), said subscriber key (SMKi) being dedicated to the authentication of a subscriber (IMSIi) within any local networks (LNj) having an agreement with the home network (HN), a key derivation function (KDF) and an algorithm to perform local authentication,
   said UICC application being further adapted to receive a network identifier (Id(LNj)) from a local network (LNj) and to use this network identifier (Id(LNj)), the key derivation function (KDF) and the subscriber key (SMKi) to derive a local key (LKi) in the UICC application of the subscriber (IMSIi), the UICC application further being adapted to use the derived

local key (LKi_{LNj}) in the algorithm to perform local authentication in the local network (LNj).

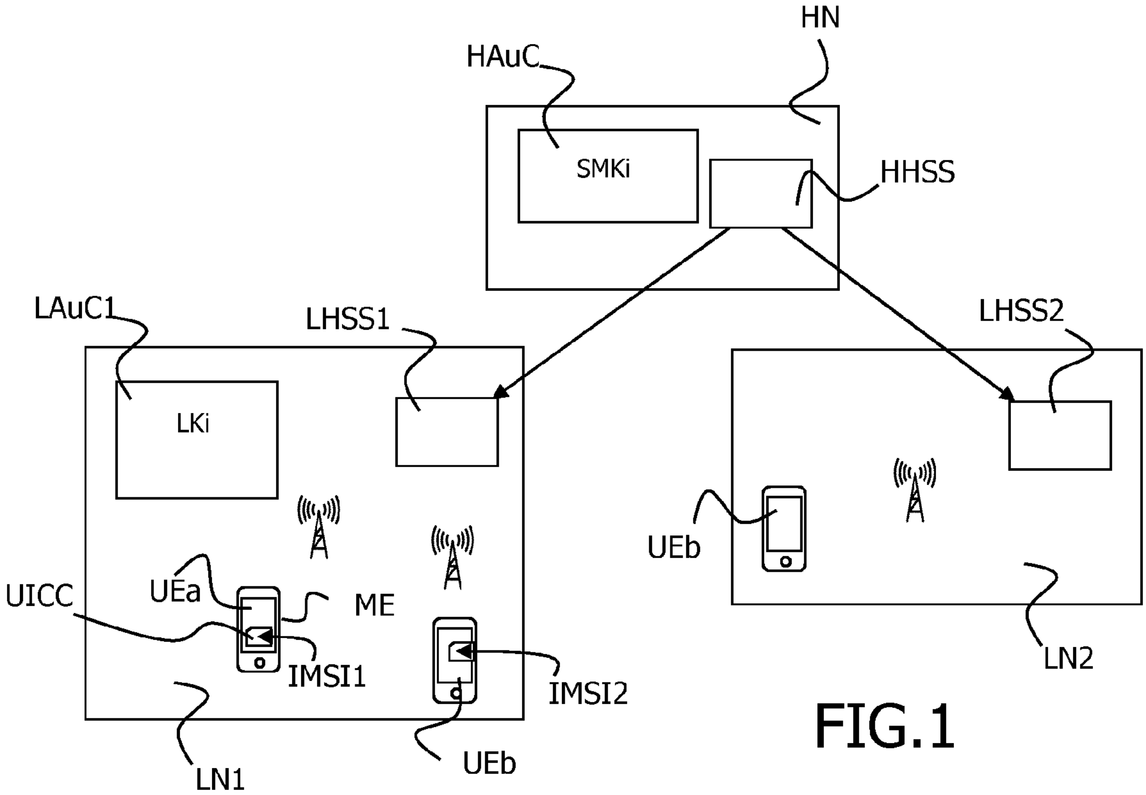
HN
HAuC
SMKi
HHSS
LAuC1
LHSS1
LHSS2
LKi
UEb
UICC
UEa
ME
IMSI1
IMSI2
LN2
LN1
UEb

FIG.1

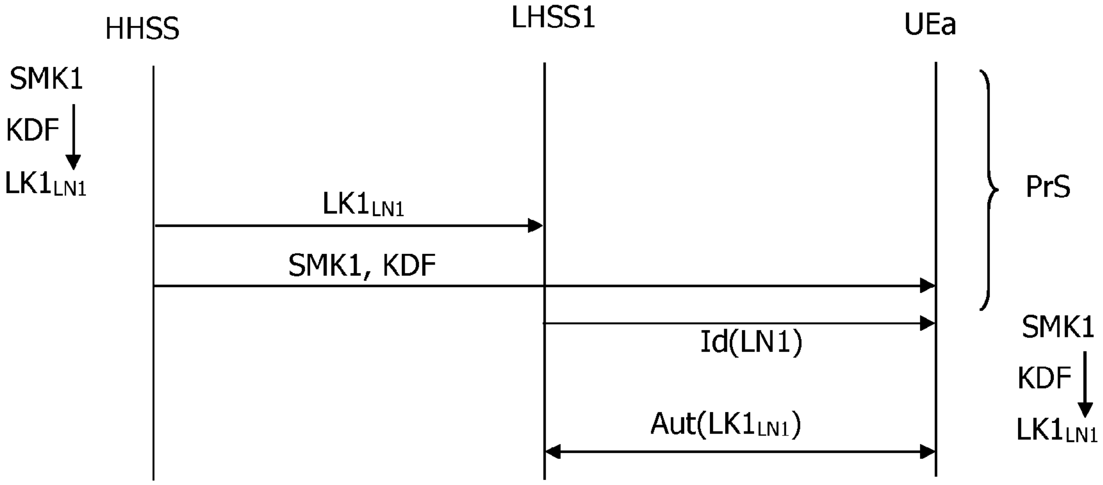
HHSS
LHSS1
UEa
SMK1
KDF
LK1LN1
LK1LN1
SMK1, KDF
PrS
Id(LN1)
SMK1
KDF
LK1LN1
Aut(LK1LN1)

FIG.2

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 15 30 6361

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	WO 2006/108907 A2 (NOKIA CORP [FI]; HAVERINEN HENRY [FI]; GINZBOORG PHILIP [FI]) 19 October 2006 (2006-10-19) * page 3 - page 20 * * page 24 - page 28 * -----	1-6	INV. H04W12/06 H04L29/06
A	GB 2 486 461 A (VODAFONE IP LICENSING LTD [GB]) 20 June 2012 (2012-06-20) * page 4 - page 5 * * page 7 - page 10 * -----	1-6	
A	WO 2014/067543 A1 (ERICSSON TELEFON AB L M [SE]) 8 May 2014 (2014-05-08) * page 5 - page 9 * -----	1-6	

TECHNICAL FIELDS SEARCHED (IPC)
H04W H04L

The present search report has been drawn up for all claims

1

Place of search	Date of completion of the search	Examiner
Munich	8 February 2016	Kraska, Nora

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons
....
& : member of the same patent family, corresponding document

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 15 30 6361

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report.
The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

08-02-2016

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2006108907 A2	19-10-2006	CN 101185311 A	21-05-2008
		EP 1875707 A2	09-01-2008
		JP 2008537398 A	11-09-2008
		KR 20070116275 A	07-12-2007
		US 2006251257 A1	09-11-2006
		WO 2006108907 A2	19-10-2006
GB 2486461 A	20-06-2012	CN 103493426 A	01-01-2014
		EP 2652898 A1	23-10-2013
		GB 2486461 A	20-06-2012
		US 2014087691 A1	27-03-2014
		WO 2012080740 A1	21-06-2012
WO 2014067543 A1	08-05-2014	CN 104756458 A	01-07-2015
		EP 2912815 A1	02-09-2015
		US 2015281958 A1	01-10-2015
		WO 2014067543 A1	08-05-2014

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82